Decision Making with Verifiable Credentials

By Edward Curran (NUCS), Paul Ezhilchelvan (NUCS), Aad Van Moorsel (NUCS) & Simon Brown (AB)

This work is an output of an ongoing Innovate UK sponsored Knowledge Transfer Partnership, involving Atom Bank (AB), Newcastle University's Computer Science department (NUCS) and Durham University's Department of Mathematical Sciences.

Please contact edward.curran@newcastle.ac.uk for enquires

Introduction

The relationship between a customer and a business often starts off with a certain degree of mutual distrust because both sides lack knowledge about the other. Long customer on-boarding journeys, tedious KYC checks and drawn out mortgage applications are all examples of several practical difficulties encountered in learning about a new customer or an existing one in a new context. Underlying them all is the same core challenge: how to use trusted sources of data to learn about the 'other' side, or counterparty, and how to justifiably decide whether or not to engage, or enhance the existing engagement, with the said counterparty. In such scenarios, trusted sources of data inevitably become vital to bootstrap a new relationship or enhance an on-going one. The use of trusted entities can thus constitute a web of trust model that drives the decision making process which, in turn, leads to justifiably correct decisions.

The paper will focus on the intersection between verifiable credentials and decision making, with an assumption that the reader is familiar with the use of verifiable credentials as a way to represent statements made by some entity (issuer, presumably trusted) about a subject, and their benefits over more traditional methods e.g. paper/pdf credentials & API connections with 3rd parties. We start by giving an overview of the problem in the context of mortgage lending and then describe a general model of decision making which is reconciled with the verifiable credentials data model [1]. Then discuss the properties of our proposed approach as well as possible implementations.

Motivation

Customer assessment forms a large component of the mortgage application process. Here the lender learns about the borrower and the property on which they are to offer a mortgage. Information is collected and assessed to make a binary decision of whether to continue or cease dealing with the applicant. The phases of information gathering and decision making are best not viewed as separate but as feeding one another in a cycle, until a final decision can be made with enough confidence to satisfy the need at hand. Confidence stems from the amount of information and to what extent it is known or trusted to be correct. This is visible in the way that a mortgage application typically includes a pre-qualification/"in principle" phase, here less accurate information is used to make a preliminary decision early on. Following it a full decision with more accurate information still needs to be made.

The lender must decide that the risk posed by the mortgage is acceptable and that the mortgage complies with their lending policy. The confidence needed in this decision is high due to the large value of the loan. In the other direction the customer is also at risk in signing up for a mortgage they do not fully understand or may not be able to afford. Mortgages are a regulated market in part to protect customers and, therefore, any mortgage lending decision made must be demonstrably compliant with regulations. For these reasons, mortgage decision making (*decisioning*) is a particularly challenging form of decision making in the context of business-customer relationships.

Our motivation is the desire to improve current mortgage decisioning and ultimately the whole property transaction process resulting in property purchase/sale. Areas we would like to see improvements in mortgage decisioning are as follows:

Speed & Ease of Use

Both the customer and lender would like decisions to be made with relative ease and no undue delays. Ease could mean minimal user interaction, e.g. for the customer, avoiding the need to repeatedly fill in forms and for the lender, using automation to reduce cost and time, etc.

Privacy

A mortgage decision by necessity involves personal customer data which is often sensitive and valuable. Decision making should follow privacy by design [2] principles such as the data minimisation to respect this.

Transparency

Regulatory compliance is an example of a need for transparency in mortgage lending decisions. Here the regulator would like to verify a decision satisfies the regulations. There exist other examples:

1. The customer could verify that any lending decisions made about them are as a result of correctly applying the lending policy to their mortgage application. Knowing they are being subjected to the same standards as everybody else creates a fair application process and promotes trust.
2. When selling mortgages on to the secondary market, as part of a mortgage securitisation, the buyer could easily verify that the originated mortgages are of a certain quality, or have a known level of risk attached to them, based on decisions that the lender has made.
3. Products often sold or supplied alongside a mortgage could take advantage of the high quality of decision making already performed during the mortgage application process.

Decision transparency should seek not to compromise customer privacy, although they appear to conflict at times.

Minimal intermediaries

Minimal intermediaries means more control for the primary parties of the relationship. It should result in simpler, more direct decision making than in the current environment where intermediaries are often used either as repositories/collators of information e.g. credit agencies or as middlemen to ease communication and coordinate the transfer of documents e.g. conveyancers, brokers, and estate agents.

Accuracy

Making correct, trusted, sources of information easily available for decision making will allow better decision models and processes to be developed. This includes guaranteeing that a decision result is not dependent on the counterparty being truthful or trusted, when this is desired.

Collaboration

An additional objective is to demonstrate how using better decision making to build a relationship with a customer can be applied not just in mortgage lending but also in the wider property transaction process. A mortgage is one piece of a full property transaction containing a large number of parties. Many relationships between these parties must be built, requiring decisions to be made,

for the transaction to proceed all the way through. Tackling the problem of building trusted relationships could demonstrate how to simplify this process for all involved.

With these goals in mind decentralised identity/web of trust and verifiable credentials were chosen as a promising option to improve decision making. The rest of the paper is an effort to create a general model of decision making using verifiable credentials with the goal to apply it to the problem described above.

Decision Making

Decision making starts with the need to make a decision, or decision requirement e.g. we need to decide whether to lend to this person. From a decision requirement we can derive a decision strategy that describes how we can reach a decision outcome that satisfies the requirement. A decision strategy consists of information requirements and decision logic. Multiple decision strategies can exist for the same decision requirement where some will be better than others in different circumstances.

An information requirement has a semantic component that describes what information is needed, and a correctness component that describes what is considered valid or correct for this piece of information. Usually the source of the information (/what entity has attested to that information being correct) is used to assess correctness. An example of an information requirement would be: we need to know income, and it must be accompanied by proof in the form of a pay slip. Correctness requirements do not necessarily have to be discrete resulting in a simple correct/incorrect, valid/not valid outcome. Instead a weighting could be assigned e.g. from 0 (incorrect) – 1 (correct). A decision strategy will usually consists of multiple information requirements. The information requirements should describe all the information that is needed by the decision logic.

The decision logic describes how the information defined in the information requirements is used to reach a decision. It could include taking into account weightings assigned as described above.

A decision strategy must then be carried out or executed. This involves gathering the information according to the requirements and applying the decision logic. Each of these could be manual or automated or any combination in between.

Decision making with verifiable credentials

Now we will attempt to align the model of decision making described so far with the verifiable credentials data model [2], with influence also from terminology used in zero knowledge proofs and anonymous credentials, including Hyperledger Indy anonymous credentials [3]

A decision strategy consists of the information requirements and decision logic as before. A single information requirement consists of a required claim, which makes up the semantic component, and a trust model that can be used to assess the correctness of that claim based on who the claim was issued by, which makes up the correctness component. The decision logic defines how the claims are used to produce a decision result. The decision result is itself a claim, or multiple claims, issued by the party that executed the decision strategy. The decision strategy will define the claim(s) that it produces.

The entity with the decision requirement is a verifier, for example a mortgage lender. The verifier uses a decision strategy to describe how the decision should be made. The verifier will request a proof, this may be multiple distinct proofs from multiple parties which the verifier collates, where the proof can be used to satisfy the decision strategy. The prover then is an entity tasked with

providing a proof to satisfy all or part of the decision strategy, this could be a borrower/mortgage customer.

The proof can take two main forms:

1. **Visible claim proof** - A set of claims, where the issuer of the claims is known (like a verifiable presentation). The verifier verifies that the claims satisfy the information requirements and applies the decision logic to create a decision result.
2. **Hidden claim proof** - A decision result accompanied by a cryptographic proof that the result was created by correctly applying the full decision strategy (including decision logic) against claims in the prover's possession. This relies on the use of zero knowledge proofs.

In both cases the prover does not have to be trusted, instead trust is placed in the decision strategy, meaning the entities defined in the trust model and in the decision logic itself. In the first instance the decision result is trusted by the verifier to be correct as they have executed the decision strategy against the claims themselves. In the second instance the decision result can be verified as correct by anybody with the proof and knowledge of the decision strategy.

Both cases have trade-offs between how much of the decision strategy must be known by the prover, and how much claim information must be known by the verifier.

In the visible claim proof: the prover learns the information requirements, as they need it to understand what claims to include in the proof. The verifier learns the exact values of claims included in the proof.
In the hidden claim proof: the prover must know the full decision strategy, as they need to be able to execute it. In return the verifier learns only that the prover is in possession of claims that produce the decision result included in the proof.

Decision Transparency with Verifiable Decisions

When we have a desire for decision transparency we define a third party, an auditor that wishes to verify that the decision result was made correctly according to a decision strategy. For example the verifier, prover and auditor could be a mortgage lender, mortgage customer/borrower and regulator respectively.

Transparency can be achieved by having the verifier commit to: the decision result, a corresponding proof and the decision strategy used. This might mean sharing it publically, or in a more select group. It is only important that the auditor accepts the commitment as valid. Ideally both the prover and verifier will commit to the decision, this is akin to signing a mortgage offer. At any point following, the auditor should be able to access the proof committed to, look up the decision strategy and verify the committed decision result corresponds to the proof and strategy. We call a decision committed to in this way a verifiable decision.

Note that there are three combinations of proofs that can be used to allow a verifier to create a verifiable decision from a decision made using one of the proof techniques described.

1. Use a visible claim proof between the prover and verifier when satisfying the decision requirement. Reuse the proof in the verifiable decision commitment. The proof can then be used by the auditor.
2. Use a hidden claim proof between prover and verifier when satisfying the decision requirement. Reuse the proof in the verifiable decision commitment. The proof can then be used by the auditor.

3. Use a visible claim proof between prover and verifier when satisfying the decision requirement. Have the verifier construct a hidden claim proof from the visible claim proof. Then include the new hidden claim proof in the commitment. The proof can then be used by the auditor.

Each of these have different trade-offs between prover claim visibility, decision logic visibility and ease of use. Approaches 1 and 3 require that the prover gives authorisation to the verifier to use their claims to allow the verifier to prove to the auditor.

It is possible for the auditor to skip out the verifier and approach the prover for verification. In the special case where the prover is also the auditor this is useful and more obvious. E.G. a prover can easily verify a decision committed to by the verifier as the prover should have all relevant claims in their possession. There is also a special case where the decision strategy the auditor wishes to verify against is not predefined. Here the verifier can commit to a visible claim proof, and allow an auditor to apply a new decision strategy on the available visible claim proof at a later date. Alternatively the auditor can pass the new decision strategy to the verifier, and the verifier can execute it on the claims they have committed to, or have in their possession, and return a hidden value proof to the auditor.

How feasible are hidden claim proofs?

A simple example of a hidden claim proof is the classic “are you 21 or older” zero knowledge proof example. Where the prover has a claim expressing their age, and they can prove they are at least 21 years old without disclosing their exact age to the verifier. In this example the semantic information requirement is a claim expressing age. The correctness information requirement might be a trust model specify the claim has to originate from the government passport office. The decision logic is “age >= 21”.

To execute the decision the decision logic must be evaluated against claims in the prover’s possession to produce a result and proof. The proof must guarantee that the claims used in the expression are unchanged since issuance, the issuers of the claims have been assessed correctly by the trust model, and that the result is the correct evaluation of the expression, using the claims in question as inputs.

This simple example requires the decision logic be expressed only as a predicate. More complicated expressions require the use of a wide range of mathematical operators. Complex decisions can be built up by combining expressions. Support for these feature in a verifiable credential system would make hidden claim proofs possible. For example currently Hyperledger Indy anonymous credentials allows a holder to create such a proof for predicate logic expressions [citation needed].

To make decision making in this manner practical we need a way to express a decision strategy such that the decision logic can be broken down into a set of expressions to be transmitted to the prover for evaluation.

Implementation

Decision Model Notation (DMN) [4] is an open standard for expressing decision models, which include decision requirements and logic. It can be used to express decision logic in Friendly Enough Expression Language (FEEL) or by describing external providers of decision logic e.g. a rule engine or a Predictive Model Mark-up Language (PMML) model.

The combination of DMN and the verifiable credentials data model could be used to express decision strategies of the type described in this paper in an open, standards based fashion. The main component missing, and required to link the two, is a format to express the trust model component, which should be executable/understandable by verifiable credential implementations. Such decision strategies would be fully executable and allow for easily reusable, privacy preserving decision making. The simplest implementations would use visible claim proofs. Decision strategies incorporating logic easily digestible into a series of expressions could be integrated with an anonymous credentials system to allow the use of hidden claim proofs. Implementations for verifiable decisions requires further investigation, but would certainly be benefited by the capability for decision making described above.

Conclusion

In this paper we have given an overview of a use cases applicable to verifiable credentials: decision making in mortgage lending. We have discussed a model of decision making incorporating verifiable credentials and identified some features such as different forms of decision proofs and notably the concept of a verifiable decision, which verifiable credentials may be uniquely position to support. Finally we ended on a brief exploration of implementation ideas.

In the future we believe that the integration of verifiable credentials with decision making tools and processes poses a great opportunity for improvement in the financial services industry, and for driving the widespread adoption of verifiable credentials.

References

[1] [Online]. Available: https://www.w3.org/TR/vc-data-model.

[2] [Online]. Available: https://rd.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf.

[3] [Online]. Available: https://github.com/hyperledger-archives/indy-anoncreds.

[4] [Online]. Available: https://www.omg.org/spec/DMN .